Volume 14, No. 3
May 2016
ISSN: 1545-679X

INFORMATION SYSTEMS EDUCATION JOURNAL

In this issue:

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published reviewed published by **ISCAP,** Information Systems and Computing Academic Professionals. The first year of publication was 2003.

ISEDJ is published online (http://isedj.org). Our sister publication, the Proceedings of EDSIGCon (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for ISEDJ.

INFORMATION SYSTEMS EDUCATION JOURNAL

Editors

ISEDJ Editorial Board

An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp

Jason M Pittman
jmpittman@cpp.edu

Ronald E. Pike
rpike@cpp.edu

California State Polytechnic University, Pomona
Pomona, CA United States

Abstract

This paper reports on the design and implementation of a cybersecurity camp offered as a cybersecurity learning experience to a group of female and male high school students. Students ranged in grade level from freshmen to senior. Student demographics, including any existing pre-requisite knowledge, were unknown to camp designers prior to the start of the camp. Such unknowns presented five design constraints that required lateral solutions to address. Chiefly, a peer learning design was deployed that allowed participants to self-organize and autonomously explore learning within secure systems administration, network security, and cryptography. Furthermore, camp participants were provided with three objects to guide the peer learning objective: a booklet containing fundamental commands within the camp knowledge areas, a Xubuntu virtual machine as a digital playground, and a digital scavenger hunt game to reinforce acquired knowledge. Observational data indicate that peer learning was a successful pedagogy. Further, the results demonstrate compelling knowledge and behavioral flows amongst participants. Accordingly, this paper goes on to suggest a Community of Practice (CofP) as an organizational umbrella to support ongoing peer learning in the cybersecurity field. The paper also calls for future research to support the development of peer learning and CofP structures to support cybersecurity education.

Keywords: Cybersecurity, education, instructional design, peer learning, virtual machine, community of practice

1.INTRODUCTION

The cybersecurity field is in a phase of explosive growth yet the news of cybersecurity exploits and resultant damage continues to dominate stories of cybersecurity success. The education community has responded with a host of related academic programs that have met with varying levels of success. In general, however, it appears that the improvements in cybersecurity education are falling short of industry demands. In fact, improvements in cybersecurity education may even be falling short of the pace of change in industry meaning that despite improvements we are falling further behind each year in meeting the needs of industry.

There are two sets of challenges for cybersecurity educators. The first of these challenges is output; we are failing to provide the number of cybersecurity professionals needed. Further, graduates lack the required depth in cybersecurity knowledge and skills as well as experience in lifelong learning to sustain careers in this fast-paced and ever-changing field. According to Kevin Mandia, a leading voice in the cybersecurity field, new entrants to the cybersecurity field require seven years of on-the-

job training before attaining a sufficient skill set to perform the duties of an information security professional (Marsh, 2012). This suggests that even the modest number of individuals trained in cybersecurity still lack the depth in skills needed to reach a productive status in a reasonable timeframe.

The second set of challenges revolves around inputs and the fact that there are too few incoming students. There is also debate as to whether the scaling efforts in academia are effective in supporting increased participation in programs. Such scaling efforts as flipped classrooms, laboratory exercises, and cybersecurity competitions struggle to accommodate mixed skill level groups with high unknowns in demographics such as age, gender and academic preparation.

The challenges in the cybersecurity field are rooted in technological and social factors that are in a state of constant development and change. As a result, cybersecurity education is partially driven by technical skills that can often be taught in an objectivist fashion, and problem solving skills that typically require a constructivist approach. Preparing students for the cybersecurity field is complicated by the array of complex topics that are represented in the field and the differing learning processes that effectively support the topics.

This paper reports on a cybersecurity camp with a focus on the inputs to cybersecurity education. The cybersecurity camp included students entering grades 9 – 12. The purpose of this observational case study was to describe the implementation of peer learning in a cybersecurity camp as a means of addressing a diverse participant sample with high-unknown academic preparation and demographics. The study may be significant for educators interested in hosting similar, STEM-based camps. As well, the results might be of interest to researchers investigating communities of practice and student-driven group dynamics within knowledge acquisition paradigms.

2. METHOD

An observational research design permitted study of participant behavior in a realistic setting (McBurney& White, 2008). As well, an observational design was appropriate as there were no pedagogical influences or treatments applied to participants (Watt & van der Berg, 2002). Further, an observational design enabled passive data collection with the goal of answering a single research question that guided the study: *how can peer learning be implemented in a cybersecurity camp when there are a high number of participant unknowns*. Accordingly, the underlying design of the cybersecurity camp targeted five primary elements.

Cybersecurity Camp Design

Design of the cybersecurity camp began approximately one month before the opening date. Design considerations included possible constraints as well as overarching goals. Design of the cybersecurity camp was constrained in five ways. Fortunately, these constraints were known before development of the camp materials. Consequently, the design of the camp included compensating features to eliminate as many undesirable learning outcomes as possible.

Design constraints

The first constraint was that the camp sponsor limited potential learning objectives to a short but broadly defined set of knowledge concepts. Limiting the learning objectives was necessary as the sponsor had scheduled additional cybersecurity camps in the near future and, as such, a number of popular learning objectives were already allocated to other institutions. Thus, the resultant design was limited to three learning objectives considered by external sources (National Information Assurance Training and Education Center, n.d.; The National Initiative for Cybersecurity Education, n.d.) as *fundamental*. In fact, as the other design constraints emerged, the importance of selecting *general* learning objectives was made more apparent. Accordingly, the learning objectives selected were secure systems administration, network security and cryptography. These learning objectives were fundamental and were considered broad enough to provide flexibility in the pedagogy for a variety of participant knowledge and skill levels.

The second constraint was the time limits associated with the camp. One time limit existed as the total number of days. Another time limit existed as the total number of hours for each day. Five days in total were allotted for the camp. However, one day was consumed for a field trip to the National Cryptologic museum while the final day was filled with closing ceremonies. The camp hours started at 9AM, and ended at 2PM. A mandatory one-hour lunch break left approximately four hours, per day, available for learning activities. These times functioned as limitations due to (a) forced scoping of knowledge material such as handouts, presentations or games; (b) the third constraint.

The third constraint was that the total number of participants was unknown prior to the camp start. Another department conducted marketing and registration. Throughout the open enrollment period, it was unclear how many community colleges had been contacted and how many students had registered.Thus, a prime design consideration was the scalability of the camp design. Both the pedagogy and the learning materials (in scope, form and function) needed to operate identically at any camp size. The danger of having too little material for the group is that participants could become bored and uninterested. On the contrary, the danger of too much material for the group is that participants could become overwhelmed and, as a result, disengaged. Naturally, the camp material needed to accommodate the average skill level of participants and be age-appropriate.

The fourth constraint was that the individual skill level of students was unknown. Knowing the average skill level of participants proved impossible without knowing the registration demographics. Accordingly, an assumption was made that participants would possess a range of skill levels with the majority possessing little knowledge in the specific topics covered in the cybersecurity camp. Yet, despite such an assumption, both the pedagogy and learning materials needed to equally serve students of low, medium, and high skill levels.

The fifth and last constraint was student gender, age, and grade level. When design of the cybersecurity camp began, the gender, age and grade level of participants were unknown. The registration process did collect such information but, due to limitations in the registration process, could not communicate the data in advance of the first camp session. As a result, the camp design necessitated incorporation of materials that would be gender, age, and grade appropriate across an array of categories.

Design goals

Based on the design constraints, five goals were established to anchor the design for the cybersecurity camp. First, peer learning would serve as the overarching pedagogy. Second, open workbooks would be used for each of the three learning days. Third, participants would have access to a Linux virtual system during the learning camp days. Fourth, each learning day would include *playtime* wherein camp participants would engage in a digital scavenger hunt. Lastly, a final presentation would reveal emergent learning concepts and afford participants the opportunity to provide overall feedback.

Peer learning

Selecting an appropriate learning theory is critical to establishing pedagogical techniques (Hill, 2002) becausethe enveloping learning theory creates a structure within which educators and learners frame knowledge.Objectivist pedagogy was not appropriate because of the high level of unknowns (Duffy &Jonassen, 1992; Jonnassen, 1991). Moreover, according to (Kaucher& Saunders, 2002), cybersecurity pedagogy should be *active*.

Peer learning was selected as the overarching pedagogy for the cybersecurity camp. Based on research (King, 2002; O'Donnell & King, 1999), peer learning was most appropriate to best compensate for the design constraints. Other constructivist pedagogies were not deemed appropriate. While consideration was given to hands-on learning via laboratory exercises, existing research demonstrated that learners do not view lab exercises as active (Pittman & Barker, 2014). Likewise, consideration was given to a pure game-based learning solution. However, game-based learning would require understanding learner skill-level ahead of the design phase if used in isolation (Prensky, 2001). Remaining constructivist pedagogies would alsonot be able to address the constraints on the camp (Moallem, 2001).

Open booklet to guide peer learning

Textbooks are objectivist in design and implementation (Keller, 2007). Thus, employing a static source of (written) knowledge would be incongruent to an implementation of constructivist peer learning. Instead, participants were provided with a medium conducive to acquisition of dynamic knowledge.

Aligned with the design goals, we furnished three booklets to all cybersecurity camp participants (examples in Table 1). The booklets were organized according to the learning goals of the cybersecurity camp: secure systems administration, network security, and cryptography. Each booklet contained an outline structure consisting of headings and knowledge points associated with the cybersecurity topic for that day.

Virtual system to explore the booklet topics

Providing a *playground* of sorts was a primary design objective for the cybersecurity camp. Digital playgrounds have been found to be motivational, competence building, and confidence enhancing (Bers, 2012; Majgaard, &Jessen, 2009). Further, pedagogical tools

operating in this context are *active* constructivist instruments.

Secure Systems Admin.	Network Security	Cryptography
Moving Around	*Moving Around*	*Did It Change?*
cd	ftp	md5
mv	ssh	sha
cp	telnet	
Working With Files	*Working with Files*	*Working with Files*
ls / ls -a	tcpdump	gpg
type	ngrep	openssl
find		
grep		

Note: Italicized phrases represent headings from booklets while non-italicized words represent knowledge points.

Table 1. *Examples of booklet headings and associated knowledge point content*.

Prior research (Pittman & Barker, 2014) established that laboratory exercises are described as objectivist in use. Accordingly, employment of the virtual systems as a companion pedagogical device to the overarching peer learning strategy required avoidance of common laboratory exercise corpora. In lieu of laboratory exercises, camp participants were encouraged to use the virtual system as an exploratory tool.

Game to reinforce peer learning

While not adequate if used alone, a game-based learning solution in conjunction with the other design goals had the potential to bolster knowledge acquisition (Prensky, 2001). Specifically, a scavenger hunt type game would give access to group play that would be internally adaptable to changing player skill (Prensky, 2001).Thus, the digital scavenger hunt consisted of 20 puzzle items, discoverable and solvable within a Xubuntu Linux virtual machine (examples in Table 2). The virtual machine was the same used during the peer-based knowledge discovery phases of the cybersecurity camp. However, access to the game portion of the cybersecurity camps occurred under a discrete login. Thus, participants' work during the playground phase each day was not accessible during game time and vice-versa.

The scavenger hunt puzzles were intended to appeal to a broad array of participant skill levels as well as to different genders. Each item required multiple steps to solve (i.e., find the correct answer). Requiring multiple steps permitted (a) an overarching trial-and-error approach and (b) all skills levels to work on the same item instead of maintaining different items for different skills levels.

Learning Goal	Clue
Secure Systems Administration	Sometimes things are that Hidden are not so hidden after all. Like an inception, there can be many layers. See if you can retrieve the password from the not so hidden.
Network Security	Fred is reliable. So reliable in fact, we were able to capture Fred logging into FTP. Can you figure out Fred's password?
Cryptography	You are stuck in the Matrix. To establish a line and call out to your operator, you need to find the key and determine the type of cipher used. Only then will you be able to rejoin the resistance.

Table 2. *Examples of scavenger hunt puzzle clues*

Participants were encouraged to work in groups and to use the knowledge captured in the booklets. Knowledgeable staff members were available to *guide* camp participants. Guidance was restricted to broad discussions of concepts and demonstrations of similar techniques. At no time were answers provided.

Presentations to convey learned concepts

The final design goal mapped to constructivist principles (Partlow& Gibbs, 2003) and provided an opportunity for cybersecurity camp participants to exercise creativity. Furthermore, presentation of cybersecurity knowledge acquired during the camp, from a pedagogical standpoint, was designed to reinforce secure systems administration, network security, and cryptography concepts that participants found meaningful. To that end, participants received a presentation template containing broad instructions. The instructions outlined the mandatory content for the presentation (four questions) but allowed participants to modify the visual content in any manner they felt necessary.

3.RESULTS

The camp started with 27 students. Two students withdrew after the first day. Twenty-five students

remained for the balance of the cybersecurity camp with full participation. Remarkably, 36% of camp attendees were female, an outcome that exceeds the typical STEM ratio of 80% male to 20% female (Beede et al., 2011). Further, a high number (40%) were non-seniors with 20% being true underclassmen (e.g., sophomore and freshmen). Figure 1 illustrates the distribution of participants by gender and grade level.

Each day, participants were allotted three hours to explore the booklets and engage in peer learning activities. Activities included group discussions, informal research, and trial-and-error practice within the same virtual machine housing the scavenger hunt. There was minimal intervention from camp staff. When necessary, assistance from staff was limited to conceptual explanations or short technical demonstrations.

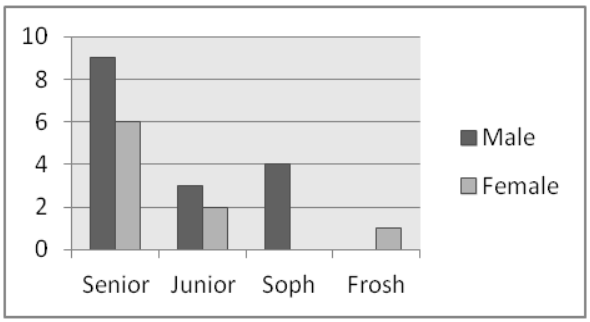

*Figure 1.*Distribution of high school student participants in the cybersecurity camp according to grade level and reported gender.

Peer Learning as Main Pedagogy

Observationally, four participants demonstrated high levels of proficiency in the camp topics. The four, highly proficient participants were not all seniors however, nor all male. Two were seniors, one was a junior and one was a sophomore. One of the junior grade level participants was female.

Figure 2 illustrates the flow of peer learning amongst participants. The four high proficiency participants emerged as focal points of knowledge for other participants. Organically, participants of moderate proficiency were observed to engage highly proficient attendees on a frequent basis. Both sides of the engagement appeared to benefit from those exchanges. Further, as the moderately proficient participants identified meaningful concepts or solved scavenger hunt puzzles, those attendees were observed to engage the less proficient participants. Thus, the moderately proficient participants served as conduits or brokers of information between highly proficient and less proficient attendees. Periodically, highly proficient participants would organize the attendees in the immediate physical area and demonstrate a new technique or knowledge concept.

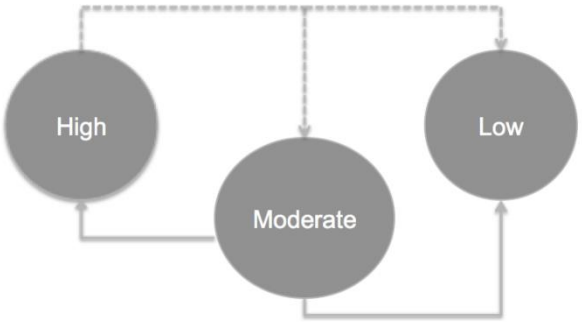

*Figure 2.*The flow of peer learning knowledge transfer between participant proficiencies.

Open Booklet to Guide Peer Learning

The open booklets appeared to be beneficial but in an unanticipated manner. The intention was for participants to add individually or group synthesized knowledge to each command in the booklets. In effect, each booklet could have turned into an approximated textbook. However, participants instead turned the booklets into what is best described as *concept maps* (Mintzes, Wandersee, & Novak, 2000).

Participants diagrammed relationships between commands within each booklet. These mappings, observationally, stemmed from knowledge acquired through group discourse. Such led to the ability for participants to sequence commands in a meaningful way during the virtual system or scavenger hunt camp phases for the respective days. As well, participants diagrammed command parameters or options across all commands within each booklet. In doing so, participants demonstrated the capacity to reuse newly synthesized knowledge.

Virtual system

Those participants that opted to work in peer groups were observed using the Xbuntu Linux system as a dynamic, ad-hoc laboratory system. While there were no pre-canned laboratory exercises included in the camp, participants organically derived a means of trial-and-error within the boundaries of collective peer knowledge. Further, the peer groups appeared to exercise a high degree of diligence in use of the open booklets to record the trial-and-error behavior. Collectively, these behaviors were consistent with the dynamics of peer learning and, observationally, appeared to facilitate knowledge acquisition and, perhaps more importantly, stimulated learning while being *fun*.

Further, knowledge gained during this phase appeared to be fed back into the open booklets. A model of such observed participant behaviors can be found in the appendix.

Presentations to Convey Concepts Learned

Participants closed out the week by presenting a summary of (a) the top cybersecurity ideas learned during the camp; (b) what camp activity was the most fun; (c) what the participant's were most proud of; (d) what area of cybersecurity they wanted to know more about; and (e) what scavenger hunt item was the peer group favorite. A content-less PowerPoint slide deck was provided as a functional outline but participants were free to modify the slide deck.

Participants self-organized into four groups that reflected the peer learning relationships established during the prior days. Each group had 15 minutes to present the group's responses (Table 2). Qualitative data, collected during, and as part of, the participant presentations were analyzed according to four thematic dimensions. Content analysis was used to mine the majority and minority perceptions within each thematic dimension.

Thematic Dimensions	**Participant Perceptions**	
	Majority Perception	*Minority Perception*
Cybersecurity Ideas Learned	Linux security	Cryptography
Most Fun Activity	Scavenger hunt	Field trip
Proudest Achievement	Linux security	Cryptography
Future Interests	Cyber attack	Cryptography

Table 3. *Participant perceptions of the CyberSTEM camp*

4.FUTURE RESEARCH

Extending the peer learning activities discussed in this paper is a daunting task. The time required to assess students learning and achievement, determine curricular supports and then deliver such curricular supports is time consuming, even in a scenario where students are doing much of the work in supporting their peers. A quick look at teams of students needing such support shows nearly 3,000 high school teams in the CyberPatriot program. Alone.CyberPatriot is only one of many cybersecurity programs at the high school level and is currently extending to middle school as well. College students in competitions such as CSAW, (Cyber Security Awareness Week) CCDC, (Collegiate Cyber Defense Competition) NCL, (National Cyber League) and ISEAGE CDC need support as well. There are tens of thousands of cybersecurity participants in need of learning support materials/activities and the numbers of such participants are growing rapidly each year.

Lave and Wenger (1991) challenged the notion that learning is the reception of knowledge and posited learning should include participation in a Community of Practice (CofP). Such communities, we believe, offer an opportunity for students to drive their own learning therefore requiring significantly less external supports. Lave and Wenger go on to call for engaging a person's intention to learn and that learning is configured as one becomes a full participant in the process. Eckert and McConnell-Ginet(1992) summarize Lave and Wenger and provide the following definition of CofP:

"An aggregate of people who come together around mutual engagement in an endeavor. Ways of doing things, ways of talking, beliefs, values, power relations – in short, practices – emerge in the course of this mutual endeavor. As a social construct, a CofP is different from the traditional community, primarily because it is defined simultaneously by its membership and by the practice in which that membership engages." (1992, p. 464)

Communities of practice are a relatively recent construct though this type of activity has been occurring since the dawn of time. It's easy to see ways that these concepts have been used for hundreds of years in medicine and many other fields. Recent publications regarding CofPs have stemmed from language development (Holmes & Meyerhoff, 1999) medicine (Ranmuthugala et al., 2011) and many others.

A benefit of using CofPs in the development of cybersecurity learners is that such learning patterns will benefit students throughout their career. It is clear from existing literature that CofPs in cybersecurity education will require unique attributes that must be developed. Particular attention must be paid to topics such as ethics and privacy which are loosely defined constructs that routinely require redefinition due to continual pressure from both technological and societal forces.

While this paper proposes the use of CofP's to support peer learning we believe there is a strong case for the use of CofP's with any teaching/learning style that involves the co-

creation of knowledge. Even with traditional teaching methodologies CofP's could be used to bring students together to create and maintain a wiki that contains the vocabulary of a course which will include students in defining the knowledge base.

Teaching methods that include students more directly in the formation and dissemination of knowledge have even greater opportunities to engage students through CofP's. For instance, the use of CTF games, cyberwar style competitions and peer learning place students in the center of knowledge production and place instructors in the role of mentors and guides. Such environments can potentially leave students floundering, however, the addition of CofP's offer students an opportunity to support one another in meeting these enhanced learning challenges. Furthermore, developing CofP's among students in school will potentially lead to CofP's in industry allowing cybersecurity practitioners to develop their field in a manner consistent with medicine and law where CofP's have been active for many years.

5. CONCLUSION

This study reported on an implementation of peer learning in the context of high school cybersecurity camp participants. The implementation leveraged five, broad design goals to overcome a high number of participant unknowns (chiefly, demographics and knowledgebase). The design included an overarching pedagogy vis-à-vis peer learning, open booklets containing fundamental commands and concepts within secure systems administration, network security, and cryptography knowledge domains. The design also included an Xbuntu Linux-based system that housed both a workspace for participants as well as a digital scavenger hunt game. An observational research design was employed to record participant interactions and behaviors relative to the design goals.

Results were positive and encouraging. Cybersecurity camp participants universally reported an increase in secure systems administration, network security, and cryptography knowledge. Overall, the peer learning strategy was successful as overall learning objectives were achieved largely because participants that were more proficient served as knowledge loci for less proficient participants.

The open booklets were useful, albeit in an unintended fashion as students used the booklets to create process maps and relationship diagrams as opposed to documenting facts in more traditional textbook fashion. Participants' appropriation of the booklets is perhaps one of the most interesting and important takeaways from the camp, as it seems to indicate their preference for making sense of knowledge in the domain.

The scavenger hunt game was the most frequently praised aspect of the camp. Peer learning, active learning and game-based learning converged in a manner conducive to participant knowledge acquisition and fun. Presentations on the final day appeared to be the second most fun part of the cybersecurity camp next to the scavenger hunt. The engagement levels made possible by the games and the peer learning context in which the games were played positively impacted learning.

6. RECOMMENDATIONS

Based on the observational results, there are three recommendations for future research. First we call for an investigation on ways that learning achievements can be quantified and recorded. Although participants reported an increase in cybersecurity knowledge, such was not quantified in this study. Future research investigating the quantitative shift in participant knowledge may be of interest to educators, researchers, employers and event designers.

Second, we call for research that explores the use of CofPs in cybersecurity and defines attributes for CofPs that are best suited to this field of study. The varying roles within cybersecurity range from topics such as privacy and ethics to technical topics such as computer networking, operating systems and hardware/software design. As such, CofPs in cybersecurity must represent a broad range of diverse topics and learning styles.

Finally, we call for research investigating the relationship between peer learning and CofPs. We posit that CofPsare an effective umbrella organizational structure to foster peer learning in cybersecurity. Such CofPs will have participants ranging in age from middle school to veteran professionals and research must examine the details of how existing expertise, age, grade level and gender may contribute to efficacy of peer learning. Individuals must enter new peer learning groups and transition between groups as their interests and external motivations cause them to venture between areas of study. CofPs must offer support mechanisms that provide an organizational umbrella over the many peer-

learning groups in the field and empower the process of transitioning between peer learning groups as needs and interests emerge.

7.REFERENCES

Beede, D., Julian, T., Langdon, D., McKittrick, G., Khan, B., &Doms, M. (2011). Women in STEM: A gender gap to innovation. ESA Issue Brief 04-11.

Donnell, A. & King, A. (1999). *Cognitive perspectives on peer learning*. Mahwah, N.J: L. Erlbaum.

Duffy, T. M. & Jonassen, D. H. (1992). *Constructivist and the technology of instruction: A conversation*, Hillsdale, NJ: Lawrence Erlbaum Associates.

Eckert, P., & McConnell-Ginet, S. (1992). THINK PRACTICALLY AND LOOK LOCALLY: Language and Gender as Community-Based Practice. *Annual Review of Anthropology*, *21*(1), 461–490.

Hill, W.F. (2002) *Learning:A survey of psychological interpretation* (7thed).Boston, MA: Allyn and Bacon.

Holmes, J., & Meyerhoff, M. (1999). The Community of Practice: Theories and methodologies in language and gender research. *Language in Society*, *28*, 173–183.

Jonnassen, D. H. (1991). Objectivist vs. constructivist: Do we need a new philosophical paradigm? *Educational Technology: Research and Development*, 39 (3), 5-14.

Kaucher, C. E., & Saunders, J.H., (2002, June). *Building an information assurance laboratory for graduate-level education*, Paper presented at 6th National Colloquium for Information System Security Education, Redmond, WA.

Keller, L. (2007). The effectiveness of teaching methods in computer programming. *In R. Carlsen et al. (Eds.), Proceedings of Society for Information Technology & Teacher Education International Conference 2007,* (820-825). Chesapeake, VA: Association for the Advancement of Computing in Education (AACE).

King, A. (2002). Structuring peer interaction to promote high-level cognitive processing, *Theory into Practice, 41*(1), 33-39. Retrieved from http://www.jstor.org/stable/1477535

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation.* New York, NY, US: Cambridge University Press. Retrieved from http://proxy.library.csupomona.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=psyh&AN=1991-98963-000&site=ehost-live&scope=site

Marsh, R. (2012, April 21). Feds need more computer defense experts, Napolitano says. Retrieved from http://security.blogs.cnn.com/2012/04/21/feds-need-more-computer-defense-experts-napolitano-says/

McBurney, D., & White, T. (2008). *Research Methods (Examples and Explanations Series)*. Cengage Learning.

Mintzes, J. J., Wandersee, J. H., & Novak, J. D. (2000). *Assessing science understanding: A human constructivist view*. San Diego: Academic Press.

Moallem, M. (2001). Applying constructivist and objectivist learning theories in the design of a web-based course: Implications for practice, *Educational Technology & Society, 4*(3). Retrieved from http://www.ifets.info/journals/4_3/moallem.html

National Information Assurance Training and Education Center. (n.d.). *Standards for Developing Curricula*. Retrieved from http://niatec.info/viewpage.aspx?id=103

Partlow, K. M., & Gibbs, W. J. (2003). Indicators of constructivist principles in internet-based courses, *Journal of Computing in Higher Education, 14*(2). 68-97. doi: 10.1007/BF02940939

Pittman, J., & Barker, H. G. (2014). Are cybersecurity laboratory exercises constructivist in use? In D. Shoemaker (Ed.), *Proceeding of the Colloquium for Information Systems Security Education: 18th Annual Conference*. San Diego, CA.

Prensky, M. (2001). *Digital game-based learning*. New York: McGraw Hill.

Ranmuthugala, G., Jennifer Plumb, Cunningham, F., Georiou, A., Westbrook, J., & Braithwaite,

J. (2011). How and why are communities of practice established in the healthcare sector? A systematic review of the literature. *BMC Health Services Research*, *11*(273). Retrieved from http://www.biomedcentral.com/1472-6963/11/273

The National Initiative for Cybersecurity Education. (n.d.). *National Cybersecurity Workforce Framework*. Retrieved from http://csrc.nist.gov/nice/framework/

Watt, J., & van der Berg, S. (2002). *Research Methods for Communication Science*.

Appendix

Model of Observed Participant Behaviors Associated with Key Peer Learning Inputs